WE CLAIM:

1. A method for multiplying an elliptic curve point Q(x,y) by a scalar to provide a point kQ, the method comprising the steps of:

   a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where ψ(Q) =λ.Q for all points Q(x,y) on the elliptic curve, and λ is an integer,

   b) establishing a representation of said scalar k as a combination of components k_i and said integer λ

   c) combining said representation and said point Q to form a composite representation of a multiple corresponding to kQ and

   d) computing a value corresponding to said point kQ from said composite representation of kQ.

2. A method according to claim 1 wherein each of said components k_i is shorter than said scalar k.

3. A method according to claim 1 wherein said components k_i are initially selected and subsequently combined to provide said scalar k.

4. A method according to claim 1 wherein said representation is of the form

   $k_i = \sum_{l=0}^{l=} k_l \lambda^i$ mod n where n is the number of points on the elliptic curve.

5. A method according to claim 4 wherein said representation is of the form $k_o + k_1$.

6. A method according to claim 1 wherein said scalar k has a predetermined value and said components k.

7. A method according to claim 3 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.

8. A method according to claim 7 wherein grouped terms G_l utilized in said simultaneous multiple addition are precomputed.

9. A method according to claim 6 wherein said components k_i are obtained by obtaining short basis vectors (u_o, u_1) of the field F, designating a vector v as (k,0), converting v from a standard, orthonomal basis to the (u_o,u_1) basis, to obtain fractions $f_o f_1$ representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ.

10. A method of generating in an elliptic curve cryptosystem a key pair having a integer k providing a private key and a public key kQ, where Q is a point on the curve,

a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda Q$ for all points Q (x,y) on the elliptic curve, λ is an integer,

b) establishing a representation of said key k as a combination of components k_i and said integer λ,

c) combining said representation and said point Q to form a composite representation of a multiple corresponding to the public key kQ and

d) computing a value corresponding to said key kQ from said composite representation of kQ.

11. A method according to claim 10 including a method according to any one of claims 2 to 9.

12. A method of computing a coordinate of a point kP on an elliptic curve resulting from a point multiplication of an initial point P by a scalar k, said method comprising the steps of:

a) decomposing said scalar k into a pair of components k_0, k_1 for point multiplication to obtain respective points on said curve which when combined provide said point kP;

b) determining a signed representation in non-adjacent form of each of said first and second components;

c) generating a table having a plurality of signed bit combinations contained in said representations and corresponding point multiples of said combinations to provide portions of said respective points;

d) establishing for each of said representations a window having a width less then the length of each of said representations;

e) initiating a sequential examination of said representations by said windows to obtain a position for one of said windows in one of said representations containing a respective one of said combinations in said table;

f) retrieving from said table the one of said point multiples corresponding to said respective one of said signed bit combinations in said table to obtain therefrom one of said portions;

g) accumulating said portion and continuing examination of said representations with a doubling of said accumulator for each bit-wise shift of said windows to obtain a representation of said coordinate of said point kP in said accumulator.

13. A method according to claim 12, wherein one of said respective points is derived from said initial point P and one of said components using an endomorphism of said curve.

14. A method according to claim 13, wherein said portions of said one of said respective points are derived from portions of the other of said respective points using said endomorphism.

15. A method according to claim 12, wherein one of said respective points is derived from said initial point P, one of said components, and a private key.

16. A method according to claim 15, wherein said portions of said respective points are precomputed and stored in said table.